You are encouraged to work on this homework together as long as you write up your own solutions. If you do so, write the names of your collaborators. Please refrain from looking up solutions to the homework on the internet or in other sources. If you must, state the source.

## Problem 1

Recall the definition of $n$-party, $r$-secret, $t$-resilient secret sharing schemes from Lecture 4. In this problem we consider secret sharing schemes over alphabet $\{0,1\}$. We call such schemes binary. Assume $n$ is sufficiently large.

(a) Show there exists a binary $n$-party, $0.1n$-secret, $0.1n$-resilient secret sharing scheme.

(b) Show there is no binary $n$-party, $0.4n$-secret, $0.4n$-resilient secret sharing scheme.

(c) **(Extra credit)** Is there a binary $n$-party, $0.3n$-secret, $0.3n$-resilient secret sharing scheme?

## Problem 2

(a) Show that the list size of the Kushilevitz-Mansour algorithm for list-decoding the Hadamard code is optimal up to constant factor. For every $\varepsilon > 0$ and sufficiently large $n$, there exists a corrupted codeword $f \in \{0,1\}^n$ so that there are at least $\Omega(1/\varepsilon^2)$ codewords of the Hadamard code $Had_n$ within relative distance $(1-\varepsilon)/2$ from $f$.

(b) Recall that the codewords of the Hadamard code can be viewed as linear functions $\ell_a(x) = \langle a, x\rangle$ from $\{0,1\}^n$ to $\{0,1\}$. The *long code* is a subcode of the Hadamard code whose codewords are only those $\ell_a$ where $a$ has hamming weight 1. These are the *dictator functions* $x_1, x_2, \ldots, x_n$. Determine the maximum number of codewords of the long code (i.e. the list size) within relative distance $(1-\varepsilon)/2$ of a corrupted codeword $f$. You need to give upper and lower bounds tight up to a constant factor. You may assume $n$ is sufficiently large.

## Problem 3

Recall that a set $S \subseteq \{0,1\}^n$ is $\varepsilon$-biased if $|\mathrm{E}_{x\sim S}[(-1)^{\langle a,x\rangle}]| \leq \varepsilon$ for every $a \neq 0$. Let $F\colon \{0,1\}^n \to [-1,1]$ and let $S$ be an $\varepsilon$-biased set.

(a) Show that

$$\left|\mathrm{E}_{x\sim\{0,1\}^n, s\sim S}[F(x)F(x+s)] - \mathrm{E}_{x,y\sim\{0,1\}^n}[F(x)F(x+y)]\right| \leq \varepsilon.$$

(**Hint:** Replace $F$ by its Fourier expansion.)

(b) Use part (a) to show that

$$\begin{aligned}\Big|\mathrm{E}_{x\sim\{0,1\}^n, s,s'\sim S}&[F(x)F(x+s)F(x+s')F(x+s+s')] \\ &- \mathrm{E}_{x,y,y'\sim\{0,1\}^n}[F(x)F(x+y)F(x+y')F(x+y+y')]\Big| \leq 2\varepsilon.\end{aligned}$$

(c) A function $f\colon \{0,1\}^n \to \{0,1\}$ is *affine* if it is a linear function or the complement of a linear function. Show that if $f$ is affine, then for all $x, y, y' \in \{0,1\}^n$, $F(x)F(x+y)F(x+y')F(x+y+y') = 1$ where $F(x) = (-1)^{f(x)}$.

(d) Show that if $\mathrm{E}_{x,y,y'\sim\{0,1\}^n}[F(x)F(x+y)F(x+y')F(x+y+y')] \geq (1-2\delta)^2$, then there exists an affine function $a$ such $\Pr[f(x) = a(x)] \geq 1-\delta$.

(e) From (b) and (d) conclude that if $\mathrm{E}_{x\sim\{0,1\}^n, s,s'\sim S}[F(x)F(x+s)F(x+s')F(x+s+s')] \geq (1-2\delta)^2 + 2\varepsilon$, then there exists an affine function $a$ such $\Pr[f(x) = a(x)] \geq 1-\delta$.

## Problem 4

Design a randomized test $T$ that, given access to two functions $F, G\colon \{0,1\}^n \to \{1,-1\}$ makes a total of 3 queries into $F$ and $G$ and behaves as follows:

- If $F = \chi_a = G$ or $F = \chi_a = -G$ for some character function $\chi_a$, then $T$ accepts $(F,G)$ with probability 1.
- For every $\varepsilon \geq 1/2$, if $T$ accepts $(F,G)$ with probability $1-\varepsilon$, then there is a character $\chi_a$ such that

$$\Pr_{x\sim\{0,1\}^n}[F(x) = \chi_a(x) = G(x)] \geq 1-2\varepsilon \text{ or } \Pr_{x\sim\{0,1\}^n}[F(x) = \chi_a(x) = -G(x)] \geq 1-2\varepsilon.$$